НОВЫЕ СРЕДСТВА
КИБЕРНЕТИКИ, ИНФОРМАТИКИ,
ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ
И СИСТЕМНОГО АНАЛИЗА

В.К. ЗАДИРАКА, А.М. КУДИН, И.В. ШВИДЧЕНКО, Б.А. БРЕДЕЛЕВ

УДК 681.3:519.72:003.26

ПРИМЕНЕНИЕ CAPTCHA В КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ

Аннотация. Описан новый подход к построению стеганографических систем с использованием теста Тьюринга для распознавания человека и компьютера (CAPTCHA). Рассмотрены общие принципы использования CAPTCHA для построения стеганографических систем в облачных компьютерных системах. Предложена стеганосистема, построенная на этих принципах. Приведены оценки ее стойкости к стеганоанализу и рассмотрены аспекты реализации.

Ключевые слова: стеганография, облачные информационно-коммуникационные системы, тест Тьюринга, CAPTCHA, общая теория оптимальных алгоритмов, радиус информации.

ВВЕДЕНИЕ

Развитие современных информационных технологий обусловливает новый подход к формированию глобальных и национальных информационно-коммуникационных систем и их безопасности. Отметим основные тенденции в этой области исследований.

1. Формирование понятия «киберпространства» с элементами независимых, распределенных в нем межнациональных, децентрализованных и анонимных сегментов, а также с «замкнутыми», национальными анклавами. Характерные примеры «подпространств» глобального киберпространства — попытки создания собственных глобальных информационно-коммуникационных систем России и Китая.

2. Разработка теоретических основ защищенных облачных технологий параллельно с возрастающим масштабом их практической эксплуатации.

3. Рост научных исследований в области создания криптографических систем для «облаков» — вычислений с зашифрованными данными (гомоморфные криптографические системы), масштабируемых и гибких систем управления ключами, защиты от новых атак на реализацию, использующих специфику построения облачных технологий.

4. Применение методов стеганографии и стеганоанализа к облачным технологиям.

Последняя тенденция особенно актуальна в связи с развитием новых аспектов использования облачных технологий, таких как «аутентификация как сервис» (AaaS), «база данных как сервис» (DaaS) и других, а также попытками внедрения систем цензуры национальных анклавов киберпространства.

СТЕГАНОГРАФИЯ В ОБЛАЧНЫХ ТЕХНОЛОГИЯХ: НОВЫЕ ВОЗМОЖНОСТИ И ОГРАНИЧЕНИЯ

Внедрение облачных технологий хранения и обработки информации не расширяет и не сужает возможности использования существующих стеганографических систем, а изменяет их. Одной из особенностей построения облачных

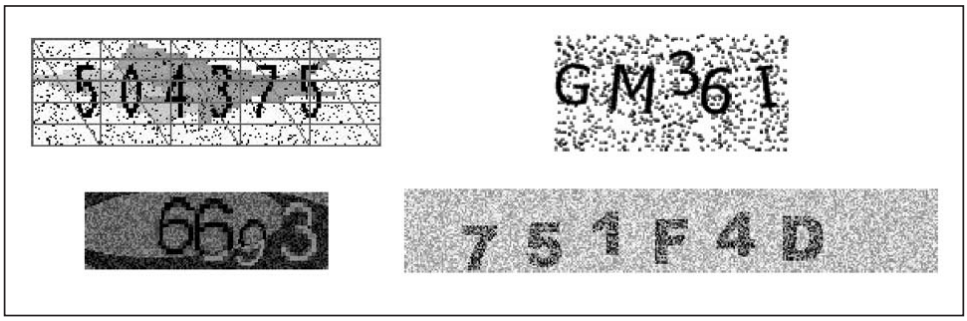

Рис. 1

сервисов хранения информации (Amazon S3, Windows Azure, Rackspace) является применение алгоритмов совместного использования хранимой информации. Их основная идея аналогична традиционному хранению информации в реляционных и полнотекстовых базах данных. При размещении новой информации в облачное хранилище (например, графического изображения) вычисляется хеш-код этих данных и сравнивается с имеющимися во избежание дублирования. При таком алгоритме размещения данных возможность использования селективного метода стеганографии существенно снижается. В то же время хранение большого количества мультимедийных данных личного пользования (не имеющих эталона) повышает возможности конструктивной стеганографии.

На сегодняшний день стеганографическая задача, такая как скрытие факта передачи сообщения от визуального обнаружения человеком, решается большинством существующих стеганографических методов (метод замены наименьшего значащего бита (НЗБ), метод дискретно-косинусного преобразования (ДКП) и др.) [1]. При этом они не всегда стойки к детектированию их использования автоматическими (компьютерными) системами [1, 2]. В современных клиент-серверных и облачных технологиях активно развивается и применяется CAPTCHA [3–5].

Термин CAPTCHA — акроним Completely Automated Public Turing test to tell Computers and Humans Apart. Основная идея теста: предложить пользователю такую задачу, которая легко решается человеком, но сложна и трудоемка для компьютера. Чаще всего в таких случаях используются задачи распознавания символов или объектов на изображении.

В наиболее распространенном варианте CAPTCHA от пользователя требуется ввести символы, изображенные, как правило, в искаженном виде на предлагаемом ему рисунке, иногда с добавлением шума или полупрозрачности (рис. 1). Реже применяются CAPTCHA, основанные на распознавании речи (например, как альтернатива для людей с нарушениями зрения) либо на других вариантах задач искусственного интеллекта.

Традиционной областью использования CAPTCHA является предотвращение множественных автоматических регистраций и отправления сообщений программами-роботами.

В то же время некоторые особенности получения CAPTCHA позволяют рассматривать их как основу для построения стеганографических систем для облачных технологий [6].

ПОСТРОЕНИЕ И ОЦЕНКА СТОЙКОСТИ СТЕГАНОСИСТЕМЫ НА ОСНОВЕ CAPTCHA

Введем некоторые понятия, необходимые для понимания последующего изложения:

AL — алфавит, используемый при выборе символов, участвующих в формировании CAPTCHA-изображения;

I — случайная последовательность символов алфавита AL длиной l: $I \in \{AL\}^l$, информационная составляющая CAPTCHA-изображения;

$RND \in \{0,1\}^w$ — двоичная случайная последовательность длиной w, используемая для искажения I, шум или шумовая составляющая CAPTCHA-изображения;

S — CAPTCHA-изображение или графический файл, содержащий информационную I и шумовую RND составляющие; CAPTCHA-изображения можно представить в форматах gif, tiff, png, jpg, размер которых измеряется в байтах.

Отметим, что для формирования качественного CAPTCHA-изображения к графическому изображению информационной составляющей I применяют различные преобразования: изменение шрифтов, размеров, цвета и трансформирование (масштабирование, поворот, наклон, искажение, растяжение, деформация, вращение, отражение и т.п.). Шумовая составляющая RND может быть в виде накладываемых на символы точек, линий, ломаных, геометрических фигур, фоновой текстуры и других различных форм, размеров и цветов. Эти элементы служат для максимизации сложности автоматического распознавания последовательности символов I.

Рассмотрим возможность использования CAPTCHA-изображения S в качестве контейнера для скрытия сообщения. Так как S — графический файл, к нему можно применить существующие стеганографические методы скрытия информации [2]. При этом есть ряд особенностей, позволяющих повысить стойкость и пропускную способность созданных на базе CAPTCHA стеганосистем.

Применение шума при формировании CAPTCHA-изображения. Шумовая составляющая имеет существенное значение для скрытия информации.

Отсутствие эталона. Вследствие уникальности формируемого CAPTCHA-изображения решается задача противодействия атаке сравнения с эталонным изображением.

Генерация контейнера под сообщение. Поскольку CAPTCHA-изображение создается уникальным для каждой последовательности символов I, можно генерировать контейнер S в зависимости от стеганосообщения. Данный вариант применим вместе с использованием ключевой стеганографии [2].

Пропускная способность стеганоканала. В файлах графического формата информационными являются три байта, определяющие цвет одной точки изображения. Так как шумовая составляющая RND может составлять более 50% всего информационного объема CAPTCHA-изображения, пропускная способность стеганоканала может превышать 50% информационного объема CAPTCHA-изображения S.

Стойкость к атакам активного нарушителя. Поскольку скрытие сообщения может осуществляться в видимую часть CAPTCHA-изображения, атаки активного нарушителя, связанные с изменением формата файла или применением алгоритма сжатия с потерями данных, будут неэффективны.

При оценке стойкости стеганосистем с использованием CAPTCHA необходимо рассматривать две модели нарушителя: стеганоаналитика-человека и автоматическую систему стеганоанализа. В первом случае стеганоаналитик знает информационную составляющую CAPTCHA-изображения, но ограничен в возможности анализа больших объемов информации, во втором — информационная часть CAPTCHA-изображения известна частично. Стеганографическую систему, использующую CAPTCHA при наличии двух перечисленных моделей нарушителя, назовем «гибридной» стеганосистемой.

В большинстве случаев стеганография предполагает использование ключа. Если это ключевая стеганосистема, то для обеспечения ее функционирования требуется построение системы управления ключами. Недостатком таких систем является организация дополнительного защищенного канала связи для постоянной передачи ключей или генерация одного ключа на множество передач. В слу-

чае использования информационной составляющей I CAPTCHA-изображения для генерации сеансового ключа возможно построение стеганосистемы, лишенной указанных недостатков.

Опишем общий алгоритм работы стеганографической системы с применением CAPTCHA.

1. Абоненты A (отправитель) и B (получатель) стеганосистемы предварительно по секретному каналу обмениваются долговременным ключом PSK. Примером отправителя может быть провайдер облачного сервиса, а получателя — пользователь облачного сервиса. Заметим, что провайдером генерируется множество CAPTCHA как содержащих, так и не содержащих скрытых сообщений (классический пример селективной стеганографии), действия абонентов по обмену скрытыми сообщениями должны синхронизироваться.

2. Отправитель A генерирует случайную последовательность символов $I \xleftarrow{random} \{AL\}^l$, которая является информационной составляющей CAPTCHA-изображения и одновременно ключевой информацией для формирования сеансового ключа стеганосистемы.

3. Отправитель A вычисляет сеансовый ключ для встраивания передаваемого сообщения M ($K_r = f_K(PSK, I)$). В качестве функции f_K может использоваться операция конкатенация $K_r = PSK \,||\, I$.

4. Отправитель A генерирует шум $RND = g(M, K_r)$ в соответствии с M и K_r длиной s_l бит.

5. Отправитель A с помощью алгоритма генерации изображения формирует CAPTCHA-изображение $S = f_{stego}(I, RND)$, которое является стеганограммой, содержащей сообщение M. Функция f_{stego} используется как для скрытия информации, так и для формирования CAPTCHA-изображения. Пример формирования S: формируем графический файл формата gif размером $8 \times s_l$ бит, представляющий изображение символов I на белом фоне. Выполняем замену каждого байта S по формуле

$$b_i = \begin{cases} 0, & \text{если} \quad RND_i = 0, \\ 255, & \text{если} \quad RND_i = 1, \end{cases}$$

где b_i — i-й байт изображения S, RND_i — i-й бит RND.

6. Получатель B (человек) распознает I по CAPTCHA-изображению S и формирует сеансовый ключ $K_r = f_K(PSK, I)$.

7. Получатель B получает RND по CAPTCHA-изображению S, используя преобразование, обратное к описанному в п. 5.

8. Получатель B по сеансовому ключу K_r и RND получает сообщение $M = g^{-1}(RND, K_r)$. Для построения функции g можно использовать метод, рассмотренный в работе [7].

Одним из важных параметров, учитываемых при проектировании и создании стеганосистемы, является пропускная способность канала передачи скрываемых сообщений. Под пропускной способностью понимают максимальное количество информации, которое может быть вложено в один элемент контейнера [2].

Связь между пропускной способностью CAPTCHA-изображения S и вероятностью P_H успешного прохождения CAPTCHA человеком определяет следующая теорема (под вероятностью прохождения CAPTCHA будем понимать вероятность правильного распознавания символов).

Теорема 1. При условии независимости распознавания символов CAPTCHA и равномерном распределении случайной величины RND пропускная способность V_S предложенной стеганосистемы обратно пропорциональна вероятности P_H прохождения CAPTCHA-изображения человеком.

Идея доказательства теоремы основана на получении оценок переменных, влияющих как на вероятность распознавания CAPTCHA человеком P_H, так и на пропускную способность V_S стеганоканала. Для оценки P_H воспользуемся следующей леммой.

Лемма 1. Верхняя граница вероятности прохождения CAPTCHA-изображения человеком определяется формулой

$$P_H = \sum_{i=j}^{m} \binom{m}{i} p^{ki} (1 - p^k)^{m-i},$$

где m — количество попыток, предоставляемых CAPTCHA, j — число попыток удачного прохождения CAPTCHA, k — количество символов в CAPTCHA.

Доказательство. Пусть C — множество битов CAPTCHA-изображения S, K — множество битов информационной составляющей I. Понятно, что $K \subset C$. Верхняя граница для значения вероятности изменения бита P_b^K при использовании описанного алгоритма в множестве K достигается при равномерном распределении шума и определяется как

$$P_b^K \le \frac{N_K}{2N_C},$$

где N_K — количество битов K, по которым происходит распознавание, N_C — количество битов C. Вероятность определения одного символа CAPTCHA-изображения выражается как некоторая убывающая функция f: $p = f(n, P_b^K)$, где n — число встраиваемых битов сообщения, определяющее связь между количеством измененных битов CAPTCHA-изображения и вероятностью ее прохождения. С увеличением числа измененных битов во множестве K вероятность прохождения CAPTCHA уменьшается. Для оценки верхней границы вероятности прохождения CAPTCHA-изображения человеком можно предположить, что символы CAPTCHA распознаются независимо один от другого. Тогда по закону Бернулли имеем

$$P_H = \sum_{i=j}^{m} \binom{m}{i} p^{ki} (1 - p^k)^{m-i}.$$

Лемма доказана.

Оценку влияния числа измененных битов во множестве K на пропускную способность V_S стеганоканала описывает следующая лемма.

Лемма 2. Увеличение пропускной способности V_S стеганоканала прямо пропорционально числу измененных битов во множестве K.

Доказательство леммы 2 следует из того, что $K \subset C$, и предположения о равномерном распределении случайной величины *RND*.

Доказательство теоремы 1 непосредственно вытекает из справедливости лемм 1 и 2.

Для получения конкретных значений пропускной способности канала и вероятности прохождения CAPTCHA проведем следующий эксперимент.

Сгенерируем девять CAPTCHA-изображений. В качестве информационной составляющей I сгенерируем случайную последовательность из шести букв латинского алфавита в разных регистрах. Отметим, что такое количество букв является средним для CAPTCHA, увеличение их количества существенно влияет на верхнюю границу вероятности прохождения P_H.

В качестве шума CAPTCHA используются точки черного цвета, распределение которых на точках изображения подчиняется равномерному закону. Цвет шума должен совпадать с цветом символов CAPTCHA, иначе процедура распоз-

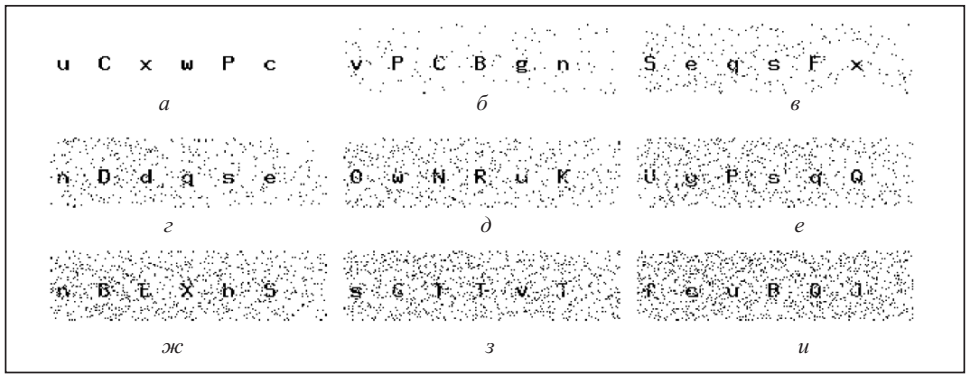

Рис. 2

Таблица 1

CAPTCHA-изображения, S (рис. 2)	Количество встраиваемых битов, n	Размер стеганоконтейнера, z (байт)	Вероятность прохождения символа, p	Верхняя граница вероятности прохождения, P_H, $m = 3$, $j = 1$	Пропускная способность стеганоканала, $U = \frac{n}{z} \cdot 100$, %
а	0	270	1	—	0
б	256	380	1	1	8.4
в	512	487	1	1	13.1
г	768	587	1	1	16.3
д	1024	666	1	1	19.2
е	1280	732	0.94	0.97	21.8
ж	1536	809	0.94	0.97	23.7
з	1792	861	0.9	0.897	26
и	2048	922	0.85	0.758	27.7

навания CAPTCHA легко автоматизируема, поскольку существует эффективный алгоритм фильтрации точек шума (при естественном предположении знания алгоритма работы CAPTCHA таким эффективным алгоритмом будет фильтрация символов CAPTCHA по коду их цвета, который отличается от кода цвета шума).

Сгенерируем ключ *PSK* длиной 10 байт как реализацию равномерно распределенной случайной величины. Сгенерируем I длиной 6 байт. Таким образом, получаем сеансовый ключ K_r длиной 16 байт путем конкатенации *PSK* и I. Для тестовых сообщений M длиной, указанной в табл. 1, генерируем *RND* длиной 30000 бит по схеме N. Provos [2]. Генерируем графический файл формата gif размером 30000 байт. С помощью графической библиотеки языка PHP формируем CAPTCHA-изображение S (рис. 2) по алгоритму, указанному выше.

Каждый сгенерированный тест решал человек. По результатам тестов путем сравнения с эталонным значением I простым подсчетом вычислялось количество неправильно распознанных символов, что и определяло вероятность p их прохождения.

Оценим пропускную способность стеганографического канала. Результаты оценки приведены в табл. 1.

Из таблицы видно, что пропускная способность стеганографического канала значительно превышает пропускную способность канала традиционных стеганосистем, основанных на методе НЗБ [2]. Кроме того, в случае использования во всем CAPTCHA-изображении пикселей с различными цветовыми значениями (не только со значением 0 и 255, как в приведенном в алгоритме примере), можно предположить, что пропускная способность канала еще увеличится.

Оценка стойкости предложенной стеганосистемы на основании известных методов [2] является трудной задачей по двум причинам: теоретико-информаци-

онные методы оценки стойкости Качина, Золнера [2] в чистом виде неприменимы, а теоретико-сложностные не учитывают факта неточного задания входных данных при автоматической модели стеганоанализа.

В гибридной модели нарушителя (человек–компьютер), рассмотренной выше, в первой модели (человек) известна часть секретного ключа стеганосистемы — I, при этом мощность множества Q (обозреваемых CAPTCHA) существенно меньше, чем во второй модели (полностью автоматической). Во второй модели часть секретного ключа I известна неполно, но мощность множества Q существенно больше, чем в первой. Отсюда можно сделать вывод, что для первой модели при известном I количество пар (S, RND) невелико, а для второй — при неточном знании I известно большое количество пар (S, RND). Стойкость стеганосистемы в данном случае определяется невозможностью отличить генераторы с равномерным распределением, зависящим от случайного значения I, и с равномерным распределением, зависящим от значения $I \,||\, M$, где распределение величины M известно и совпадает с распределением встраиваемых сообщений. Если функция g построена на базе симметричного блочного шифра, например AES, то задача оценки стойкости стеганосистемы в первой модели нарушителя существенно зависит от стойкости симметричного блочного шифра, которая исследована.

Оценка стойкости во второй модели усложняется тем, что вследствие неполного знания I ключ K_r зависит не только от долговременного ключа PSK, но и от некоторой случайной величины E_r, определяемой алгоритмом CAPTCHA (погрешностью распознавания CAPTCHA). Учитывая тот факт, что в стеганосистеме, использующей CAPTCHA, сочетаются алгоритм распознавания образов и генератор шума в графическом изображении, создающий исходные данные, «наихудшие» для алгоритма CAPTCHA, для оценки стойкости стеганосистемы во второй модели нарушителя можно применить подход, предложенный в [8].

Теорема 2. Стойкость стеганографической системы, работа которой описывается приведенным алгоритмом, определяется радиусом информации алгоритма генерации CAPTCHA-изображения.

Для доказательства теоремы представим стеганосистему как совокупность множеств (C, S, M, K, Q) соответственно контейнеров, стеганограмм, открытых сообщений, ключей и сообщений, наблюдаемых нарушителем. Для встраивания сообщения используется оператор $E : C \times M \times K \to N(C) = Q$. Его можно также рассматривать в виде $E_{K \times M} : C \to N(C)$, где $M \times K$ — составной ключ. Тогда стеганосистема может рассматриваться как криптосистема с составным ключом, оператор $Dt : C \times \Re_+ \to 2^M$, где $\Re_+ = [0, \infty)$ — оператор стеганоанализа. Построение модели стеганосистемы осуществляется аналогично построению модели криптосистемы. Пусть оператор стеганоанализа обладает двумя свойствами:

$$Dt(c, 0) \neq \varnothing \quad \forall c \in C, \tag{1}$$

$$\delta_1 \le \delta_2 \Rightarrow Dt(c, \delta_1) \subset Dt(c, \delta_2) \quad \forall \delta_1, \delta_2 \in \Re_+, \; c \in C. \tag{2}$$

Для заданного значения $\varepsilon \ge 0$ элемент $c \in C$, удовлетворяющий условию $c \in Dt(c, \varepsilon)$, называется ε-приближением. Задача поиска ε-приближения решается при отсутствии полной информации об элементе c, о нем известна некоторая информация $N(c) = q \in Q$, где $N : C \to Q$ — информационный оператор или информация о контейнерах (заполненных и пустых), которой владеет нарушитель. Зная q, необходимо найти ε-приближение к $m \in Dt(c, 0)$. Поскольку условия (1), (2) выполняются для любого метода стеганографического анализа, к определенной таким образом модели стеганосистемы возможно применить результаты, полученные в рамках общей теории оптимальных алгоритмов [9].

Рассмотрим множество $V(N, c) = \{\widetilde{c} \in C : N(\widetilde{c}) = N(c)\}$ всех элементов $\widetilde{c}$, не отличимых с помощью информационного оператора $N(c)$. Если оператор N не биекция, то множество $V(N, c)$ неодноточечное. Можно считать, что множест-

во $V(N, c)$ является классом эквивалентности на множестве Q, а разбиение контейнеров на классы эквивалентности порождает информационный оператор N, который называется неполным оператором. Оператор стеганоанализа, примененный к неполному информационному оператору, порождает множество $A(N, c, \varepsilon) = \bigcap_{\tilde{c} \in V(N,c)} Dt(\tilde{c}, \varepsilon)$. Согласно условию (2) величины $r(N, c) = \inf\{\delta : A(N, c, \delta) \neq \varnothing\}$ и $r(N) = \sup_{c \in C} r(N, c)$ определяют нижние оценки точности решений, которые могут быть достигнуты при неполном информационном операторе.

Используя результаты работы [9], получаем, что на классе идеальных алгоритмов $\Phi(N) : Q \to M$, с введенными определениями локальной $e(\varphi, N, c) = \inf\{\delta : \varphi(Q) \in A(N, c, \delta)\}$ и глобальной $e(\varphi, N) = \sup_{c \in C} e(\varphi, N, c)$ погрешностями (φ — алгоритм реализации оператора стеганоанализа), информация Q позволяет найти ε-приближение для произвольного $c \in C$ тогда и только тогда, когда выполняется одно из условий:

$$r(N) < \varepsilon,\ r(N) = \varepsilon,\ \exists \varphi : \varphi(Q) \in Dt(c, e(\varphi, N))\ \ \forall c \in C.$$

Таким образом, для оценки стойкости к стеганоанализу можно использовать радиус информации, определяемый как алгоритмом генерации шума CAPTCHA-изображения, так и алгоритмом стеганоанализа, использующим как составную часть алгоритм распознавания CAPTCHA. Из того факта, что оба алгоритма являются составляющими алгоритма генерации CAPTCHA-изображения, следует доказательство теоремы.

ЗАКЛЮЧЕНИЕ

Исследование характеристик стеганографических систем, использующих особенности облачных информационно-коммуникационных систем, показывает их определенные преимущества перед традиционными системами. Широкое применение «в облаках» CAPTCHA позволяет построить гибридные (относительно модели нарушителя) стеганографические системы, характеризующиеся большей пропускной способностью стеганоканала по сравнению с другими стеганосистемами.

СПИСОК ЛИТЕРАТУРЫ

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. — М.: СОЛОН-ПРЕСС, 2009. — 265 с.
2. Задирака В.К., Кудин А.М. Особенности реализации криптографических и стеганографических систем по принципу облачных вычислительных технологий // Искусственный интеллект. — 2012. — № 3. — С. 438–444.
3. CAPTCHA: Telling humans and computer apart automatically. — http://www.captcha.net/captcha_cacm.pdf.
4. Wagner N.R. CAPTCHAs and information hiding. — http://www.cs.utsa.edu/~wagner/captcha/hiding12.pdf.
5. Shirali-Shahreza M., Shirali-Shahreza M.H. A new solution for password key transferring in steganography methods by CAPTCHA through MMS technology // Proc. of the First Intern. Conf. on Information and Emerging Technologies (ICIET 2007) , Karachi, Pakistan, July 6–7, 2007. — P. 137–142.
6. Задирака В.К., Кудин А.М., Швидченко И.В. Стеганография в облачных информационно-коммуникационных системах // Компьютерная математика. — 2014. — № 1. — С. 54–60.
7. Provos N. Defending against statistical steganalysis // Proc. of the 10th USENIX security symp., Washington. — Aug., 2001. — P. 323–335.
8. Кудин А.М. Математическая модель стеганографической системы на базе общей теории оптимальных алгоритмов // Математичне та комп'ютерне моделювання: Зб. наук. праць Кам'янець-Подільського нац. ун-ту та Інституту кібернетики ім. В.М. Глушкова. — Кам.-Под.: Вид-во. Кам.-Под. нац. ун-ту, 2010. — № 4. — С. 136–143.
9. Трауб Д., Васильковский Г., Вожьняковский Х. Информация, неопределенность, сложность. — М.: Мир, 1988. — 184 с.

Поступила 11.02.2015